RECEIVED
CENTRAL FAX CENTER

MAR 17 2006

Allen, Dyer, Doppelt,
Milbrath & Gilchrist, P.A.
------ INTELLECTUAL PROPERTY ATTORNEYS ------

255 South Orange Avenue • Suite 1401 • Orlando, FL 32801
Mail to: P. O. Box 3791 • Orlando, FL 32802-3791
tel: 407-841-2330 • fax: 407-841-2343
cobrien@addmg.com

FACSIMILE COVER SHEET

TO: Examiner Tongoc Tran – United States Patent and Trademark Office: Art Unit 2134

CLIENT NAME/NUMBER: 51211

TELEPHONE: 571-272-3061 **FAX NO:** 571-273-8300

FROM: Cian G. O'Brien **DATE:** March 17, 2006

NUMBER OF PAGES (INCLUDING COVER SHEET): 35

COMMENTS/INSTRUCTIONS:

Please see attached Appeal Brief in reply to the Examiner's Office Action of December 20, 2005 for U.S. Patent Application Serial No. 09/761,173.

MAR 17 2006

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF APPEALS

In re Patent Application of: **DELLMO, ET AL.**	
Serial No. **09/761,173**	Examiner: **T.TRAN**
Filing Date: **JANUARY 16, 2001**	Art Unit: **2134**
For: **SECURE WIRELESS LAN DEVICE INCLUDING TAMPER RESISTANT FEATURE AND ASSOCIATED METHODS**	Attorney Docket No. **51211**

APPELLANT'S APPEAL BRIEF

MS Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

The Commissioner is hereby authorized to charge the Appeal Brief filing fee in the amount of $500.00 to Deposit Account No. **08-0870**. The Commissioner is authorized to charge or credit any discrepancies in fee amounts to Deposit Account No. **08-0870**.

(1) Real Party in Interest

The real party in interest is Harris Corporation, assignee of the present application as recorded at Reel 011660, Frame 0096.

(2) Related Appeals and Interferences

At present there are no related appeals or interferences.

(3) Status of the Claims

Claims 1-51 are pending in the application. Claims 1-51 are rejected and are being appealed herein.

In Re Patent Application of:
DELLMO, ET AL.
Serial No: **09/761,173**
Filing Date: **JANUARY 16, 2001**

(4) Status of the Amendments

At present there are no related appeals or interferences.

(5) Summary of the Claimed Subject Matter

With reference to FIGS. 1-7 (FIGS. 1 and 7 reproduced below) and the associated description at page 7, line 3 through page 15, line 32, of the present application, for example, the invention is intended to provide a secure wireless LAN device **20** that provides greater security, and yet without a significant increase in cost and/or complexity. The device **20** includes a housing **21**, which carries a connector **27** at one end and a pair of antennas **22** at the opposite end. The interface connector **27** may be a PCMCIA connector or other similar connector that can readily interface to a number of possible LAN devices, such a corresponding PC-card slot in the side of a laptop computer **25**, for example.

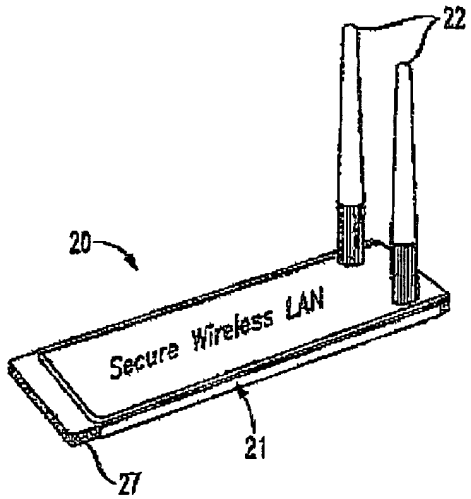


FIG. 1 of the present application

In Re Patent Application of:
DELLMO, ET AL.
Serial No: **09/761,173**
Filing Date: **JANUARY 16, 2001**

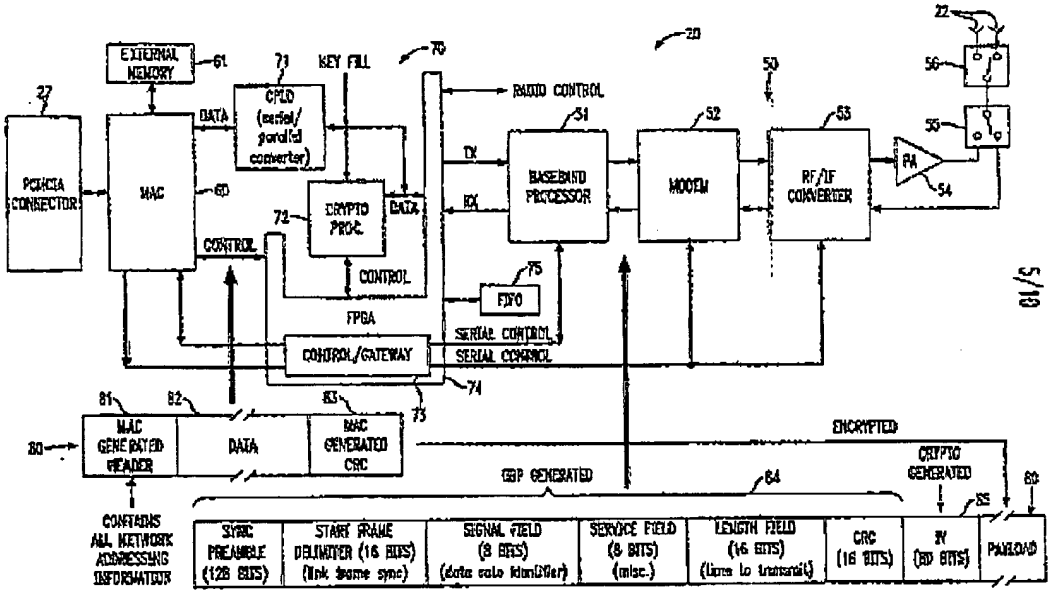


FIG. 7 of the present application

Independent Claim 1 is directed to a secure wireless local area network (LAN) device **20** including a housing **21**, and a wireless transceiver **50**, media access controller (MAC) **60** and cryptography circuit **70** each carried by the housing, the cryptography circuit connected to the MAC and the wireless transceiver. The cryptography circuit **70** operates using cryptography information and renders unusable the cryptography information based upon tampering.

Independent Claim 13 is directed to a secure wireless local area network (LAN) device **20** including a housing **21**, and a wireless transceiver **50**, cryptography circuit **70**, and at least one connector **27** each carried by the housing, the at least one connector for connecting a LAN station **25** and/or a LAN access point **30**. The cryptography

circuit 70 is connected to the wireless transceiver 50, operates using cryptography information and renders unusable the cryptography information based upon tampering.

Independent Claim 24 is directed to a secure wireless local area network (LAN) device 20 comprising a housing 21, and a wireless transceiver 50, media access controller (MAC) 60, and cryptography circuit 70 each carried by the housing, the cryptography circuit connected to the MAC and the wireless transceiver. The cryptography circuit 70 comprising at least one volatile memory 107 for storing the cryptography information, and a battery 109 for maintaining the cryptography information in the at least one volatile memory.

Independent Claim 30 is directed to a secure wireless local area network (LAN) device 20 including a housing 21, and a wireless transceiver 50, at least one connector 27, and a cryptography circuit 70 each carried by the housing, the at least one connector for connecting to a LAN station 25 and/or a LAN access point 30. The cryptography circuit 70 comprises at least one volatile memory 107 for storing the cryptography information, and a battery 109 for maintaining the cryptography information in the at least one volatile memory.

Independent Claim 36 is directed to a secure wireless local area network (LAN) system 45 including a plurality of LAN devices 25 and a respective secure wireless LAN device 20 connected to each LAN device. Each secure wireless LAN device 20 includes a housing 21, with a wireless transceiver 50 and cryptography circuit 70 each carried by the housing, the cryptography circuit connected to the wireless transceiver. The cryptography circuit 70 operates using cryptography information and renders unusable the cryptography information based upon tampering.

In Re Patent Application of:
DELLMO, ET AL.
Serial No: **09/761,173**
Filing Date: **JANUARY 16, 2001**

Independent Claim 46 is directed to a method for making tamper resistant a secure wireless local area network (LAN) device **20** comprising a housing **21**, a wireless transceiver **50** carried by the housing and a cryptography circuit **70** carried by the housing. The method comprises storing cryptography information in the cryptography circuit **70** and rendering unusable the cryptography information based upon tampering with the secure wireless LAN device **20**.

For the reasons set forth in the arguments below, the independent Claims 1, 13, 24, 30, 36 and 46 and their respective dependent claims stand separately as groups defined as follows: Claims 1-12 stand as a group, Claims 13-23 stand as a group, Claims 24-29 stand as a group, Claims 30-35 stand as a group, Claims 36-45 stand as a group and Claims 46-51 stand as a group.

(6) Grounds of Rejection to be Reviewed On Appeal

Claims 1-6, 8, 10, 13-18, 21, 24-28, 30-34, 36-41 and 43-50 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Treadway et al. (U.S. Patent No. 6,480,477) in view of Schneck et al. (U.S. Patent Publication No. 2001/0021926) and Bambridge et al. (U.S. Patent No. 6,259,933).

Claims 7, 9, 19-20, 29, 35, 42 and 51 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Treadway et al. in view of Schneck et al. and Bambridge et al., and further in view of Baldwin et al. (U.S. Patent No. 6,560,448).

Claims 11 and 22 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Treadway et al. in view of Schneck et al. and Bambridge et al., and further in view of Soliman (U.S. Patent Publication No. 2002/0114288).

Claims 12 and 23 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Treadway et al. in view of

In Re Patent Application of:
DELLMO, ET AL.
Serial No: **09/761,173**
Filing Date: **JANUARY 16, 2001**

Schneck et al. and Bambridge et al., and further in view of Treadway et al. '285 (U.S. Patent No. 6,665,285).

(7) Argument

A. Independent Claim 1 And Its Dependent Claims Are Patentable

The Examiner rejected independent Claim 1 as being unpatentable over Treadway et al. in view of Schneck et al. and Bambridge et al. The Treadway et al. patent discloses wireless terminals **100**, **100'** communicating over a wireless link **102** carrying mega-bits-per-second data packets. (Column 5, lines 65-67; Column 6, lines 29-31; See FIG. 1 reproduced below). The terminal **100** includes an outdoor unit (ODU) **104** housing a MAC **222'** including an encryption/decryption block **612** between a rate control logic **250'** and rate buffer **252'** (See FIG. 16 reproduced below).

As recited above, independent Claim 1 is directed to a secure wireless local area network (LAN) device **20** including a housing **21**, and a wireless transceiver **50**, media access controller (MAC) **60** and cryptography circuit **70** each carried by the housing, the cryptography circuit **70** connected to the MAC **60** and the wireless transceiver **50**. The cryptography circuit **70** operates using cryptography information and renders unusable the cryptography information based upon tampering.

In Re Patent Application of:
DELLMO, ET AL.
Serial No: **09/761,173**
Filing Date: **JANUARY 16, 2001**

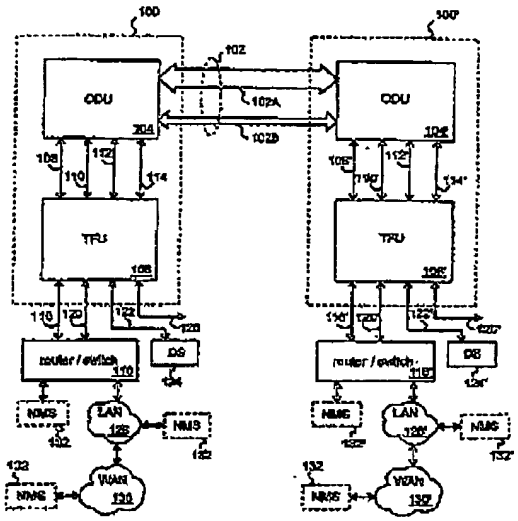


FIG. 1 of Treadway et al.

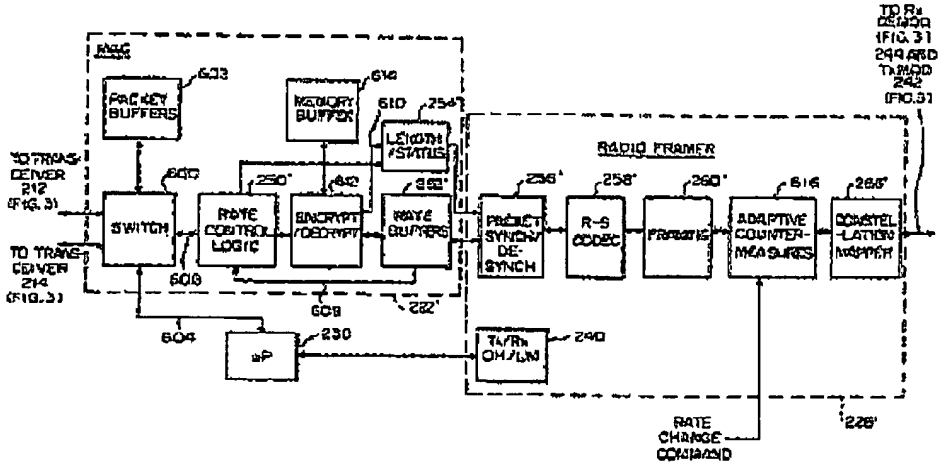


FIG. 16 of Treadway et al.

In Re Patent Application of:
DELLMO, ET AL.
Serial No: **09/761,173**
Filing Date: **JANUARY 16, 2001**

The rate control logic **250** of the Treadway et al. patent measures the length of each data packet to be transmitted over the link **102**, and stores the data packet length and status (too short, too long, misaligned) in a length/status buffer **254**. (Column 11 lines 51-55; Column 12, lines 9-14). For encryption, the encryption/decryption block **612** encrypts data packets prior to storing them in the rate buffers **252'** and decrypts data packets received from the link **102** (Column 23, lines 50-55). To ensure a constant rate of transmission over the link **102**, upon the rate buffer **252'** filling with data packets causing a slow transmission rate over the link **102**, the rate control logic **250'** sends a pause packet to a switch **600** so to queue incoming data packets in packet buffers **602'** for a predetermined time. (Column 23, lines 34-41). The encryption/decryption block **612** uses a control signal line **610** to instruct the length/status buffer **254'** to provide an encryption tag, or encryption key for the data packet, to the packet synch/de-synch block **256'** resulting in an encryption tag field **702** in the reformed data packet **700** (Column 23, lines 59-67; Column 24, lines 8-10).

The Examiner correctly acknowledges that the Treadway et al. patent does not disclose a MAC carried by a housing, and cites to the Bambridge et al. patent to provide such. The Examiner further correctly acknowledges that the Treadway et al. patent does not disclose a cryptography circuit connected to a MAC and wireless transceiver, where the cryptography circuit operates using cryptography information rendered unusable based upon tampering. The Examiner looks to the Schneck et al. patent to provide this noted deficiency.

The Schneck et al. patent discloses a distributor **102** having an authoring mechanism **112** for encrypting data **106** into packaged data **108** having an encrypted body part **120** and encrypted rules **124** for accessing the data (Paragraph 87, 94).

In Re Patent Application of:
DELLMO, ET AL.
Serial No: 09/761,173
Filing Date: JANUARY 16, 2001

Upon payment **110** to the distributor **102**, the encrypted data **108** and rules **124** are distributed to the user **104** (Paragraph 126; See FIG. 1 reproduced below).

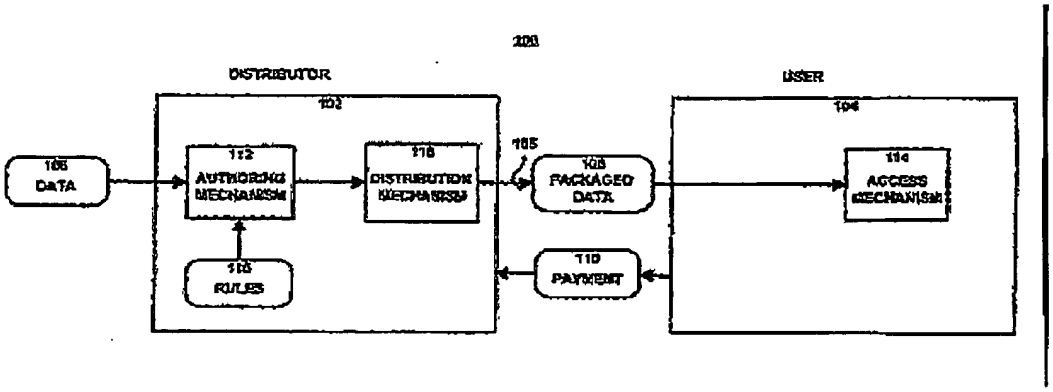


FIG. 1 of Schneck et al.

The user **104** has an access mechanism **114** confined within a security boundary **167** containing required components for tamper detection for the destruction of all internal data (Paragraph 132, 134; See FIG. 8). Protected data is secured through tamper detection employing physical confinement within an access mechanism **114**, such as a sealed-unit laptop computer. (Paragraph 62, 134-135). The access mechanism **114** decrypts the encrypted rules **124** and grants the user access to the protected data (Paragraph 129, 163, 168, 170). The packaged data **108** includes computer software, text, graphics, audio, and video, alone or in combination (Paragraph 52). The access mechanism **114** may alternatively be used as a co-processor for plugging into the main board of a computer **170**, the computer passing control to the access mechanism for accessing controlled data. (Paragraph 136; See FIG. 9 reproduced below).

In Re Patent Application of:
DELIMO, ET AL.
Serial No: **09/761,173**
Filing Date: **JANUARY 16, 2001**

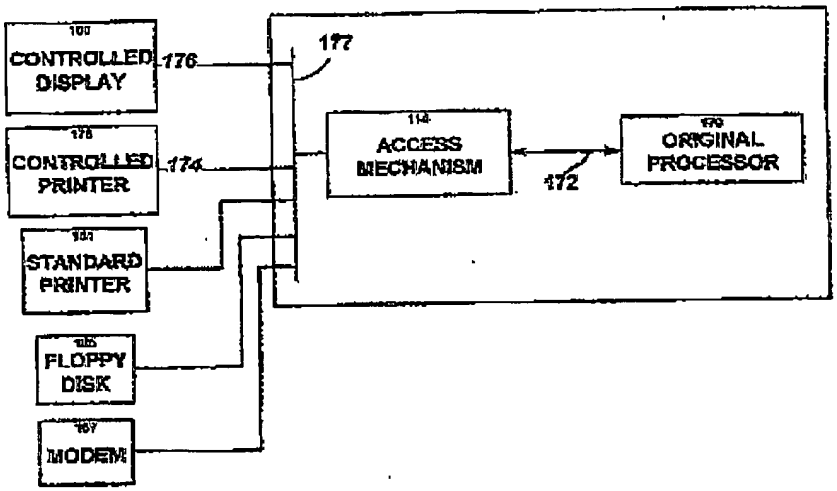


FIG. 9 of Schneck et al.

In the Final Official Action, the Examiner contends that it would have been obvious to one of ordinary skill in the art at the time of the present invention to incorporate the co-processor (ie. access mechanism **114**) tamper detection feature for destroying cryptographic information of the Schneck et al. patent with the Treadway et al. cryptographic apparatus to protect the cryptographic information from tampering. It is respectfully suggested that one of ordinary skill in the art at the time of the present invention would have been taught away from making the suggested combination. More specifically, the encryption/decryption block **612** of the Treadway et al. patent teaches dual encryption and decryption of Ethernet data packets to and from the wireless data link **102**. However, as the authoring mechanism **112** of Schneck et al. encrypts the data **106** into the encrypted packaged data **108**, and thus the access mechanism **114** decrypts pre-encrypted packaged data **108**, the access mechanism **114** teaches away from

mutual encryption/decryption of data packets, as required by the Treadway et al. patent. Although the access mechanism **114** includes private keys, such keys are solely used for decryption, as asserted by the Examiner on pages 2-3 of the Final Official Action. Thus, one of skill in the art would be taught away from combining the teachings of the access mechanism **114** (co-processor) tampering device with the Treadway et al. encryption/decryption block **612**, as such teaching suggests removing the encryption of data packets while still maintaining their decryption.

More specifically, the Treadway et al. patent teaches storing encrypted data packets within a memory buffer **614**, rate buffers **252'**, and packet synch **256'**, as well as encryption keys within the length/status buffer **254'**. The Treadway et al. patent includes no teaching or suggestion to destroy such information, as suggested by the access mechanism **114** tampering device of the Schneck et al. patent (Paragraph 134). Due to the steady stream of data packets incoming to the MAC **222'**, even destroying the information in these buffers would nevertheless result in reformed data packets **700** without the encryption tag field **702** supplied by the length/status buffer **254'** to be outputted over the wireless data link **102**. Contrary to the Schneck et al. teaching of confining all data within the access mechanism **114** tampering device for deletion of all internal data upon tampering, the steady stream of data packets of the Treadway et al. patent cannot be so confined and deleted. Appellants submit that such a combination would destroy the operability of the Treadway et al. patent, and yield a result contrary to the teaching of the Schneck et al. patent access mechanism **114** tampering device.

Further, the Treadway et al. patent includes no teaching or suggestion to combine the memory buffer **614**, rate buffers **252'**, packet synch **256'**, and length/status buffer **254'**

within an enclosure with a processing unit, tamper detect mechanism, and the other "required" components of the access mechanism **114** illustrated in FIG. 8. In fact, the Treadway et al. specifically teaches that the packet synch **256'** and the other components are within separate MAC **222'** and radio framer **228'** units, thus teaching away such a combination. Since the Treadway et al. patent includes a continuous data flow system for signalling various components to ensure a continuous data flow rate across the wireless link **102**, one of ordinary skill in the art would be discouraged from combining the data packets or components within a closed, confined housing as suggested by the access mechanism **114** of the Schneck et al. patent.

As previously discussed, the Schneck et al. patent teaches an access mechanism **114** (co-processor) tampering mechanism protecting data via physical confinement within a sealed-unit laptop computer. Appellants submit that such teaching is completely contrary to the Treadway et al. Ethernet data packet transmission between terminals (frequently among laptop computers). Thus, one of ordinary skill in the art at the time of the present invention would be discouraged from combining the access mechanism **114** (co-processor) with the encryption apparatus of the Treadway et al. patent, requiring the encryption of Ethernet data packets be transmitted between network terminals.

Additionally, Appellants further submit that there is no motivation or teaching to combine the references as suggested by the Examiner. As described above, the Treadway et al. patent relates to the encryption/decryption of Ethernet data packets transmitted at a megabit-per-second rate over a wireless LAN link and includes no suggestion or motivation to combine with a tampering detection mechanism for packaged data sold to a user and secured within the physical bounds of an

access laptop computer.

The Treadway et al. patent further includes no suggestion or motivation to combine with a co-processor requiring connection to a computer **170**, particularly as the encryption/decryption block **612** does not disclose such a computer connection. Appellants further re-emphasizes that the Treadway et al. patent requires an encryption/decryption process for signalling the length/status buffer **254'** containing length/status information of each data packet. Indeed, there is no suggestion or motivation to combine the co-processor of the Schneck et al. patent in such an encryption/decryption process, particularly as the co-processor does not process Ethernet data packets, and thus cannot generate a required signal to a length/status buffer **254'** containing length/status information of Ethernet data packets.

Consequently, Appellants respectfully submit that there is no proper motivation to selectively combine the three cited references. The Appellants respectfully submit that the Examiner is using impermissible hindsight, gleaned from the Appellants' own specification, as a motivation to selectively combine disjointed pieces of the prior art in an attempt to produce the claimed invention.

As the Examiner is aware, to establish a prima facie case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the reference itself or in the knowledge generally available to one of ordinary skill in the art, to modify the reference. Second, there must be a reasonable expectation of success. Finally, the prior art reference must teach or suggest all the claim features. The initial burden is on the Examiner to provide some suggestion of the desirability of doing what the Appellants have done. To support the conclusion that the

claimed invention is directed to obvious subject matter, either the reference must expressly or impliedly suggest the claimed invention or the Examiner must present a convincing line of reasoning as to why the artisan would have found the claimed invention to have been obvious in light of the teachings of the reference. Both the suggestion to make the claimed combination and the reasonable expectation of success must be founded in the prior art and not in Appellants' disclosure.

There is simply no teaching or suggestion in the cited references to provide the combination of features as claimed. Accordingly, for at least the reasons given above, Appellants maintain that the cited references do not disclose or fairly suggest the invention as set forth in independent Claim 1. Furthermore, no proper modification of the teachings of these references could result in the invention as claimed. Thus, the rejection under 35 U.S.C. §103(a) should be withdrawn or reversed.

Accordingly, independent Claim 1 is patentable, and the dependent claims, which recite yet further distinguishing features of the invention, are also patentable, and require no further discussion.

B. Independent Claim 13 And Its Dependent Claims Are Patentable

The Examiner rejected independent Claim 13 as being unpatentable over Treadway et al. in view of Schneck et al. and Bambridge et al. The Treadway et al., Schneck et al. and Bambridge et al. patents are discussed above.

As recited above, independent Claim 13 is directed to a secure wireless local area network (LAN) device 20 including a housing 21, and a wireless transceiver 50, cryptography circuit 70, and at least one connector 27 each

carried by the housing, the at least one connector for connecting to at least one of a LAN station **25** and a LAN access point **30**. The cryptography circuit **70** is connected to the wireless transceiver **50**, and operates using cryptography information and renders unusable the cryptography information based upon tampering.

On Pages 5-6 of the Final Official Action, the Examiner asserts that independent Claim 13 includes recitations "substantially similar" to independent Claim 1 and rejects independent Claim 13 based on the similar rationale.

Appellants submit that the claim recitation of at least one connector **27** each carried by the housing for connecting to at least one of a LAN station **25** and a LAN access point **30** is a claim recitation that cannot be simply ignored by the Examiner. In rejecting dependent Claim 8 including the same recitation, the Examiner cites to column 3, lines 35-50 and column 27, lines 28-40 of the Treadway et al. patent. However, these portions of the Treadway et al. patent merely discuss radio super frames **380** communicating with nodes of a metropolitan area network, and fail to disclose a connector **27** carried by the housing for connecting to at least one of a LAN station **25** and a LAN access point **30**. Thus, even if the suggested combination of the Treadway et al. and the Schneck et al. patents was obvious, it would nevertheless fail to produce the claimed invention.

As argued above with respect to independent Claim 1, Appellants respectfully contend that one of ordinary skill in the art at the time of the present invention would be taught away from incorporating the teaching of the co-processor tampering mechanism of the Schneck et al. patent with the encryption/decryption block **612** of the Treadway et al. patent, as suggested by the Examiner. As further discussed above with regard to independent Claim 1, there is no suggestion or

teaching in the Treadway et al. patent to combine the co-processor tampering mechanism of the Schneck et al. patent with the encryption/decryption block **612** of the Treadway et al. patent, as suggested by the Examiner.

Accordingly, independent Claim 13 is patentable, and the dependent claims, which recite yet further distinguishing features of the invention, are also patentable, and require no further discussion.

C. Independent Claim 24 And Its Dependent Claims Are Patentable

The Examiner rejected independent Claim 24 as being unpatentable over Treadway et al. in view of Schneck et al. and Bambridge et al. The Treadway et al., Schneck et al. and Bambridge et al. patents are discussed above.

As recited above, independent Claim 24 is directed to a secure wireless local area network (LAN) device **20** comprising a housing **21**, and a wireless transceiver **50**, media access controller (MAC) **60**, and cryptography circuit **70** each carried by the housing, the cryptography circuit connected to the MAC and the wireless transceiver. The cryptography circuit **70** comprising at least one volatile memory **107** for storing the cryptography information, and a battery **109** for maintaining the cryptography information in the at least one volatile memory.

On Page 6 of the Final Official Action, the Examiner asserts that independent Claim 24 includes recitations "substantially similar" to independent Claim 1 and rejects independent Claim 24 based on the similar rationale.

Appellants submit that the claim recitation of at least one volatile memory **107** for storing the cryptography information, and a battery **109** for maintaining the cryptography information in the at least one volatile memory

is a claim recitation that cannot be simply ignored by the Examiner. In rejecting dependent Claim 2 including the same recitation, the Examiner cites to paragraph 67 of the Schneck et al. patent to provide such. However, this portion of the Schneck et al. patent discloses a long-life battery for **rewriting** over the private key for decrypting protected data in a nonvolatile memory, thus teaching away a battery for **maintaining** cryptographic information in a volatile memory, as recited in independent Claim 24. Thus, even if the suggested combination of the Treadway et al. and the Schneck et al. patents was obvious, it would nevertheless fail to produce the claimed invention.

As argued above with respect to independent Claim 1, Appellants respectfully contend that one of ordinary skill in the art at the time of the present invention would be taught away from incorporating the teaching of the co-processor tampering mechanism of the Schneck et al. patent with the encryption/decryption block **612** of the Treadway et al. patent, as suggested by the Examiner. As further discussed above with regard to independent Claim 1, there is no suggestion or teaching in the Treadway et al. patent to combine the co-processor tampering mechanism of the Schneck et al. patent with the encryption/decryption block **612** of the Treadway et al. patent, as suggested by the Examiner.

Accordingly, independent Claim 24 is patentable, and the dependent claims, which recite yet further distinguishing features of the invention, are also patentable, and require no further discussion.

D. Independent Claim 30 And Its Dependant Claims Are Patentable

The Examiner rejected independent Claim 30 as being unpatentable over Treadway et al. in view of Schneck et al.

and Bambridge et al. The Treadway et al., Schneck et al. and Bambridge et al. patents are discussed above.

As recited above, independent Claim 30 is directed to a secure wireless local area network (LAN) device **20** including a housing **21**, and a wireless transceiver **50**, at least one connector **27**, and a cryptography circuit **70** each carried by the housing, the at least one connector **27** for connecting to at least one of a LAN station **25** and a LAN access point **30**. The cryptography circuit **70** comprises at least one volatile memory **107** for storing the cryptography information, and a battery **109** for maintaining the cryptography information in the at least one volatile memory.

On Page 6 of the Final Official Action, the Examiner asserts that independent Claim 30 includes recitations "substantially similar" to independent Claim 1 and rejects independent Claim 30 based on the similar rationale.

Appellants submit that the claim recitations of at least one connector **27** each carried by the housing for connecting to at least one of a LAN station **25** and a LAN access point **30** is a claim recitation that cannot be simply ignored by the Examiner. In rejecting dependent Claim 8 including the same recitation, the Examiner cites to column 3, lines 35-50 and column 27, lines 28-40 of the Treadway et al. patent. However, these portions of the Treadway et al. patent merely discuss radio super frames **380** communicating with nodes of a metropolitan area network, and fail to disclose a connector **27** carried by the housing for connecting to at least one of a LAN station **25** and a LAN access point **30**. Thus, even if the suggested combination of the Treadway et al. and the Schneck et al. patents was obvious, it would nevertheless fail to produce the claimed invention.

Appellants submit that the claim recitation of at least one volatile memory **107** for storing the cryptography

information, and a battery 109 for maintaining the cryptography information in the at least one volatile memory is a claim recitation that cannot be simply ignored by the Examiner. In rejecting dependent Claim 2 including the same recitation, the Examiner cites to paragraph 67 of the Schneck et al. patent to provide such. However, this portion of the Schneck et al. patent discloses a long-life battery for **rewriting** over the private key for decrypting protected data in a nonvolatile memory, thus teaching away a battery for **maintaining** cryptographic information in a volatile memory, as recited in independent Claim 30. Thus, even if the suggested combination of the Treadway et al. and the Schneck et al. patents was obvious, it would nevertheless fail to produce the claimed invention.

As argued above with respect to independent Claim 1, Appellants respectfully contend that one of ordinary skill in the art at the time of the present invention would be taught away from incorporating the teaching of the co-processor tampering mechanism of the Schneck et al. patent with the encryption/decryption block 612 of the Treadway et al. patent, as suggested by the Examiner. As further discussed above with regard to independent Claim 1, there is no suggestion or teaching in the Treadway et al. patent to combine the co-processor tampering mechanism of the Schneck et al. patent with the encryption/decryption block 612 of the Treadway et al. patent, as suggested by the Examiner.

Accordingly, independent Claim 30 is patentable, and the dependent claims, which recite yet further distinguishing features of the invention, are also patentable, and require no further discussion.

E. Independent Claim 36 And Its Dependant Claims Are Patentable

In Re Patent Application of:
DELLMO, ET AL.
Serial No: **09/761,173**
Filing Date: **JANUARY 16, 2001**

The Examiner rejected independent Claim 36 as being unpatentable over Treadway et al. in view of Schneck et al. and Bambridge et al. The Treadway et al., Schneck et al. and Bambridge et al. patents are discussed above.

As recited above, independent Claim 36 is directed to a secure wireless local area network (LAN) system **45** including a plurality of LAN devices **25**, a respective secure wireless LAN device **20** connected to each of said plurality of LAN devices, each secure wireless LAN device including a housing **21**, with a wireless transceiver **50** and cryptography circuit **70** each carried by the housing, the cryptography circuit **70** connected to the wireless transceiver **50**. The cryptography circuit **70** operates using cryptography information and renders unusable the cryptography information based upon tampering.

On Page 6 of the Final Official Action, the Examiner asserts that independent Claim 36 includes recitations "substantially similar" to independent Claim 1 and rejects independent Claim 36 based on the similar rationale.

As argued above with respect to independent Claim 1, Appellants respectfully contend that one of ordinary skill in the art at the time of the present invention would be taught away from incorporating the teaching of the co-processor tampering mechanism of the Schneck et al. patent with the encryption/decryption block **612** of the Treadway et al. patent, as suggested by the Examiner. As further discussed above with regard to independent Claim 1, there is no suggestion or teaching in the Treadway et al. patent to combine the co-processor tampering mechanism of the Schneck et al. patent with the encryption/decryption block **612** of the Treadway et al. patent, as suggested by the Examiner.

Accordingly, independent Claim 36 is patentable, and the dependent claims, which recite yet further distinguishing

features of the invention, are also patentable, and require no further discussion.

F. Independent Claim 46 And Its Dependant Claims Are Patentable

The Examiner rejected independent Claim 46 as being unpatentable over Treadway et al. in view of Schneck et al. and Bambridge et al. The Treadway et al., Schneck et al. and Bambridge et al. patents are discussed above.

As recited above, independent Claim 46 is directed to a method for making tamper resistant a secure wireless local area network (LAN) device **20** comprising a housing **21**, a wireless transceiver **50** carried by the housing and a cryptography circuit **70** carried by the housing, the method comprising storing cryptography information in the cryptography circuit **70** and rendering unusable the cryptography information based upon tampering with the secure wireless LAN device.

On Page 6 of the Final Official Action, the Examiner asserts that independent Claim 46 includes recitations "substantially similar" to independent Claim 1 and rejects independent Claim 46 based on the similar rationale.

As argued above with respect to independent Claim 1, Appellants respectfully contend that one of ordinary skill in the art at the time of the present invention would be taught away from incorporating the teaching of the co-processor tampering mechanism of the Schneck et al. patent with the encryption/decryption block **612** of the Treadway et al. patent, as suggested by the Examiner. As further discussed above with regard to independent Claim 1, there is no suggestion or teaching in the Treadway et al. patent to combine the co-processor tampering mechanism of the Schneck et al. patent with the encryption/decryption block **612** of the Treadway et

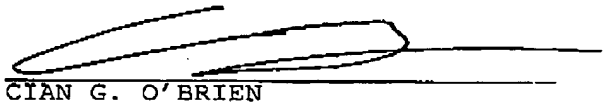
al. patent, as suggested by the Examiner.

Accordingly, independent Claim 46 is patentable, and the dependent claims, which recite yet further distinguishing features of the invention, are also patentable, and require no further discussion.

CONCLUSIONS

In view of the foregoing arguments, it is submitted that all of the claims are patentable over the prior art. Accordingly, the Board of Patent Appeals and Interferences is respectfully requested to reverse the earlier unfavorable decision by the Examiner.

Respectfully submitted,



CIAN G. O'BRIEN
Reg. No. 55,792
Allen, Dyer, Doppelt, Milbrath
& Gilchrist, P.A.
255 S. Orange Avenue, Suite 1401
Post Office Box 3791
Orlando, Florida 32802
Telephone: 407/841-2330
Fax: 407/841-2343
Attorney for Appellant

In Re Patent Application of:
DELLMO, ET AL.
Serial No: **09/761,173**
Filing Date: **JANUARY 16, 2001**

CERTIFICATE OF FACSIMILE TRANSMISSION

I hereby certify that this correspondence is being forwarded via facsimile no. 571-273-8300 to MS Appeal Brief-Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on this 17th day of March, 2006.

Melissa Shazian

RECEIVED
CENTRAL FAX CENTER

MAR 17 2006

In Re Patent Application of:
DELLMO, ET AL.
Serial No: 09/761,173
Filing Date: JANUARY 16, 2001

APPENDIX A - CLAIMS ON APPEAL
FOR U.S. PATENT APPLICATION SERIAL NO. 09/761,173

1. A secure wireless local area network (LAN) device comprising:

a housing;

a wireless transceiver carried by said housing;

a media access controller (MAC) carried by said housing; and

a cryptography circuit carried by said housing and connected to said MAC and said wireless transceiver, said cryptography circuit operating using cryptography information and rendering unuseable the cryptography information based upon tampering.

2. A secure wireless LAN device according to Claim 1 wherein said cryptography circuit comprises:

at least one volatile memory for storing the cryptography information; and

a battery for maintaining the cryptography information in said at least one volatile memory.

3. A secure wireless LAN device according to Claim 2 wherein said cryptography circuit further comprises at least one switch operatively connected to said housing for disconnecting said battery from said at least one volatile memory so that the cryptography information therein is lost based upon breach of said housing.

4. A secure wireless LAN device according to Claim 1 wherein said cryptographic information comprises a cryptography key.

5. A secure wireless LAN device according to Claim

1 wherein said security information comprises at least a portion of a cryptography algorithm.

6. A secure wireless LAN device according to Claim 1 wherein said MAC implements a predetermined wireless LAN MAC protocol.

7. A secure wireless LAN device according to Claim 6 wherein said predetermined wireless LAN MAC protocol is based upon the IEEE 802.11 standard.

8. A secure wireless LAN device according to Claim 1 further comprising at least one connector carried by said housing for connecting to at least one of a user station and an access point.

9. A secure wireless LAN device according to Claim 8 wherein said at least one connector comprises a PCMCIA connector.

10. A secure wireless LAN device according to Claim 1 wherein said cryptography circuit comprises:

a cryptography processor; and

a control and gateway circuit connecting said cryptography processor to said MAC and said wireless transceiver.

11. A secure wireless LAN device according to Claim 1 wherein said wireless transceiver comprises:

a baseband processor;

a modem connected to said baseband processor; and

a radio frequency transmitter and receiver connected to said modem.

In Re Patent Application of:
DELLMO, ET AL.
Serial No: **09/761,173**
Filing Date: **JANUARY 16, 2001**

12. A secure wireless LAN device according to Claim 1 further comprising at least one antenna carried by said housing and connected to said wireless transceiver.

13. A secure wireless local area network (LAN) device comprising:

a housing;

a wireless transceiver carried by said housing;

at least one connector carried by said housing for connecting to at least one of a LAN station and a LAN access point; and

a cryptography circuit carried by said housing and connected to said wireless transceiver, said cryptography circuit operating using cryptography information and rendering unuseable the cryptography information based upon tampering.

14. A secure wireless LAN device according to Claim 13 wherein said cryptography circuit comprises:

at least one volatile memory for storing the cryptography information; and

a battery for maintaining the cryptography information in said at least one volatile memory.

15. A secure wireless LAN device according to Claim 14 wherein said cryptography circuit further comprises at least one switch operatively connected to said housing for disconnecting said battery from said at least one volatile memory so that the cryptography information therein is lost based upon breach of said housing.

16. A secure wireless LAN device according to Claim 13 wherein said cryptographic information comprises a cryptography key.

17. A secure wireless LAN device according to Claim 13 wherein said security information comprises at least a portion of a cryptography algorithm.

18. A secure wireless LAN device according to Claim 13 further comprising a media access controller (MAC) carried by said housing; and wherein said MAC implements a predetermined wireless LAN MAC protocol.

19. A secure wireless LAN device according to Claim 18 wherein said predetermined wireless LAN MAC protocol is based upon the IEEE 802.11 standard.

20. A secure wireless LAN device according to Claim 13 wherein said at least one connector comprises a PCMCIA connector.

21. A secure wireless LAN device according to Claim 13 wherein said cryptography circuit comprises:

a cryptography processor; and

a control and gateway circuit connecting said cryptography processor to said MAC and said wireless transceiver.

22. A secure wireless LAN device according to Claim 13 wherein said wireless transceiver comprises:

a baseband processor;

a modem connected to said baseband processor; and

a radio frequency transmitter and receiver connected to said modem.

23. A secure wireless LAN device according to Claim 13 further comprising at least one antenna carried by said housing and connected to said wireless transceiver.

24. A secure wireless local area network (LAN) device comprising:

a housing;

a wireless transceiver carried by said housing;

a media access controller (MAC) carried by said housing; and

a cryptography circuit carried by said housing and connected to said MAC and said wireless transceiver, said cryptography circuit comprising

at least one volatile memory for storing the cryptography information, and

a battery for maintaining the cryptography information in said at least one volatile memory.

25. A secure wireless LAN device according to Claim 24 wherein said cryptography circuit further comprises at least one switch operatively connected to said housing for disconnecting said battery from said at least one volatile memory so that the cryptography information therein is lost based upon a breach of said housing.

26. A secure wireless LAN device according to Claim 24 wherein said cryptographic information comprises a cryptography key.

27. A secure wireless LAN device according to Claim 24 wherein said security information comprises at least a portion of a cryptography algorithm.

28. A secure wireless LAN device according to Claim 24 wherein said MAC implements a predetermined wireless LAN MAC protocol.

29. A secure wireless LAN device according to Claim 28 wherein said predetermined wireless LAN MAC protocol is based upon the IEEE 802.11 standard.

30. A secure wireless local area network (LAN) device comprising:

a housing;

a wireless transceiver carried by said housing;

at least one connector carried by said housing for connecting to at least one of a LAN station and a LAN access point; and

a cryptography circuit carried by said housing and connected to said wireless transceiver, said cryptography circuit comprising

at least one volatile memory for storing the cryptography information, and

a battery for maintaining the cryptography information in said at least one volatile memory.

31. A secure wireless LAN device according to Claim 30 wherein said cryptography circuit further comprises at least one switch operatively connected to said housing for disconnecting said battery from said at least one volatile memory so that the cryptography information therein is lost based upon breach of said housing.

32. A secure wireless LAN device according to Claim 30 wherein said cryptographic information comprises a cryptography key.

33. A secure wireless LAN device according to Claim 30 wherein said security information comprises at least a portion of a cryptography algorithm.

In Re Patent Application of:
DELLMO, ET AL.
Serial No: **09/761,173**
Filing Date: **JANUARY 16, 2001**

34. A secure wireless LAN device according to Claim 30 further comprising a media access controller (MAC) carried by said housing; and wherein said MAC implements a predetermined wireless LAN MAC protocol.

35. A secure wireless LAN device according to Claim 34 wherein said predetermined wireless LAN MAC protocol is based upon the IEEE 802.11 standard.

36. A secure wireless local area network (LAN) system comprising:

a plurality of LAN devices;

a respective secure wireless LAN device connected to each of said plurality of LAN devices, each secure wireless LAN device comprising

a housing,

a wireless transceiver carried by said housing, and

a cryptography circuit carried by said housing and connected to said wireless transceiver, said cryptography circuit operating using cryptography information and rendering unuseable the cryptography information based upon tampering.

37. A secure wireless LAN system according to Claim 36 wherein said cryptography circuit comprises:

at least one volatile memory for storing the cryptography information; and

a battery for maintaining the cryptography information in said at least one volatile memory.

38. A secure wireless LAN system according to Claim 37 wherein said cryptography circuit further comprises at least one switch operatively connected to said housing for disconnecting said battery from said at least one volatile memory so that the cryptography information therein is lost

based upon breach of said housing.

39. A secure wireless LAN system according to Claim 36 wherein said cryptographic information comprises a cryptography key.

40. A secure wireless LAN system according to Claim 36 wherein said security information comprises at least a portion of a cryptography algorithm.

41. A secure wireless LAN system according to Claim 36 wherein said secure wireless LAN device comprises a media access controller (MAC) connected to said wireless transceiver; and wherein said MAC implements a predetermined wireless LAN MAC protocol.

42. A secure wireless LAN system according to Claim 41 wherein said predetermined wireless LAN MAC protocol is based upon the IEEE 802.11 standard.

43. A secure wireless LAN system according to Claim 36 wherein said plurality of LAN devices comprises a plurality of user stations.

44. A secure wireless LAN system according to Claim 36 wherein said plurality of LAN devices comprises at least one user station and at least one access point.

45. A secure wireless LAN system according to Claim 36 wherein said plurality of LAN devices comprises a plurality of access points.

46. A method for making tamper resistant a secure wireless local area network (LAN) device comprising a housing,

a wireless transceiver carried by the housing and a cryptography circuit carried by the housing, the method comprising:

storing cryptography information in the cryptography circuit; and

rendering unuseable the cryptography information based upon tampering with the secure wireless LAN device.

47. A method according to Claim 46 wherein the cryptography circuit comprises at least one volatile memory for storing the cryptography information, and a battery for maintaining the cryptography information in the at least one volatile memory; and wherein rendering unuseable comprises disconnecting the battery from the at least one volatile memory based upon a breach of the housing.

48. A method according to Claim 46 wherein the cryptographic information comprises a cryptography key.

49. A method according to Claim 46 wherein the security information comprises at least a portion of a cryptography algorithm.

50. A method according to Claim 46 wherein the secure wireless LAN device further comprises a media access controller (MAC) carried by the housing; and wherein the MAC implements a predetermined wireless LAN MAC protocol.

51. A method according to Claim 50 wherein the predetermined wireless LAN MAC protocol is based upon the IEEE 802.11 standard.

In Re Patent Application of:
DELLMO, ET AL.
Serial No: 09/761,173
Filing Date: JANUARY 16, 2001

APPENDIX B - EVIDENCE APPENDIX PURSUANT TO 37 C.F.R. § 41.37(c)(1)(ix)

None.

In Re Patent Application of:
DELLMO, ET AL.
Serial No: **09/761,173**
Filing Date: **JANUARY 16, 2001**

APPENDIX C - RELATED PROCEEDINGS APPENDIX PURSUANT TO 37 C.F.R. § 41.37(c)(1)(x)

None.

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☒ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☒ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.